ICSA-200

ISA Security Compliance Institute – IIoT Component Security Assurance –

ISASecure ICSA chartered laboratory operations and accreditation

Version 1.1

December 2022

A. DISCLAIMER

ASCI and all related entities, including the International Society of Automation (collectively, “ASCI”) provide all materials, work products and, information (‘SPECIFICATION’) AS IS, WITHOUT WARRANTY AND WITH ALL FAULTS, and hereby disclaim all warranties and conditions, whether express, implied or statutory, including, but not limited to, any (if any) implied warranties, duties or conditions of merchantability, of fitness for a particular purpose, of reliability or availability, of accuracy or completeness of responses, of results, of workmanlike effort, of lack of viruses, and of lack of negligence, all with regard to the SPECIFICATION, and the provision of or failure to provide support or other services, information, software, and related content through the SPECIFICATION or otherwise arising out of the use of the SPECIFICATION. Also, there is no warranty or condition of title, quiet enjoyment, quiet possession, correspondence to description, or non-infringement with regard to the SPECIFICATION.

Without limiting the foregoing, ASCI disclaims all liability for harm to persons or property, and users of this SPECIFICATION assume all risks of such harm.

In issuing and making the SPECIFICATION available, ASCI is not undertaking to render professional or other services for or on behalf of any person or entity, nor is ASCI undertaking to perform any duty owed by any person or entity to someone else. Anyone using this SPECIFICATION should rely on his or her own independent judgment or, as appropriate, seek the advice of a competent professional in determining the exercise of reasonable care in any given circumstances.

B. EXCLUSION OF INCIDENTAL, CONSEQUENTIAL AND CERTAIN OTHER DAMAGES

To the maximum extent permitted by applicable law, in no event shall ASCI or its suppliers be liable for any special, incidental, punitive, indirect, or consequential damages whatsoever (including, but not limited to, damages for loss of profits or confidential or other information, for business interruption, for personal injury, for loss of privacy, for failure to meet any duty including of good faith or of reasonable care, for negligence, and for any other pecuniary or other loss whatsoever) arising out of or in any way related to the use of or inability to use the SPECIFICATION, the provision of or failure to provide support or other services, information, software, and related content through the SPECIFICATION or otherwise arising out of the use of the SPECIFICATION, or otherwise under or in connection with any provision of this SPECIFICATION, even in the event of the fault, tort (including negligence), misrepresentation, strict liability, breach of contract of ASCI or any supplier, and even if ASCI or any supplier has been advised of the possibility of such damages.

C. OTHER TERMS OF USE

Except as expressly authorized by prior written consent from the Automation Standards Compliance Institute, no material from this document owned, licensed, or controlled by the Automation Standards Compliance Institute may be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, except for non-commercial use only, provided that you keep intact all copyright and other proprietary notices. Modification of the materials or use of the materials for any other purpose, such as creating derivative works for commercial use, is a violation of the Automation Standards Compliance Institute’s copyright and other proprietary rights.

Revision history

version	date	changes
1.1	2022.12.04	Initial version published to https://www.isasecure.org/

Contents

List of requirements

List of tables

FOREWORD

This is one of a series of documents that defines the ISASecure® ICSA (IIoT Component Security Assurance) certification program for IIoT (Industrial Internet of Things) devices and gateways. These product types are defined in the present specification. They are subtypes of one of the product types: embedded devices, host devices and network devices, defined in the standard IEC 62443-4-2. ISASecure ICSA is developed and managed by the industry consortium ISA Security Compliance Institute (ISCI). The current list of all ISASecure certification programs and documents related to these programs can be found on the web site https://www.ISASecure.org.

1 Scope

The ISASecure® certification programs have been developed by an industry consortium called the ISA Security Compliance Institute (ISCI) with a goal to accelerate industry wide improvement of cyber security for Industrial Automation and Control Systems (IACS). An organization that performs evaluations and grants certifications under the ISASecure ICSA (Industrial Internet of Things Component Security Assurance) program is referred to as a *ISASecure ICSA chartered laboratory*, or (more briefly) a *chartered laboratory*. This document specifies the criteria and processes that define:

- Requirements on the operations of a chartered laboratory (Section 6); and
- How a chartered laboratory shall begin and continue ISASecure IIoT component certification operations (Section 7).

ISCI has based its certification program approach on:

- International standards for conformity assessment programs
- IACS security standards IEC 62443-4-1 and IEC 62443-4-2 (also published as ANSI/ISA standards)
- Specifications developed for the ISASecure ICSA program.

This document provides a complete reference to these sources, and details ISASecure ICSA program-specific requirements for compliance with applicable general specifications and standards.

ISASecure ICSA is a *product* certification program for IIoT devices and IIoT gateways. These two IIoT component types are defined in 3.1 of the present document.

IIoT devices and IIoT gateways are subtypes of the IACS component types embedded device, host device, and network device. defined in [IEC 62443-4-2]. ISCI also has developed *product* certification and *process* certification programs for:

- IACS component products, the ISASecure CSA program (Component Security Assurance)
- Control system products, the ISASecure SSA program (System Security Assurance)
- Supplier's secure product development lifecycle process, the ISASecure SDLA program (Security Development Lifecycle Assurance).

The separate documents CSA-200 *ISASecure CSA chartered laboratory operations and accreditation*, SSA-200 *ISASecure SSA chartered laboratory operations and accreditation* and SDLA-200 *ISASecure SDLA chartered laboratory operations and accreditation* address these same topics as they relate to chartered laboratories that perform ISASecure CSA, SSA and SDLA certifications, respectively.

Since an IIoT device or IIoT gateway can be classified under one or more of the IACS component types defined in the 62443 standard, it is also certifiable under the CSA program. The CSA and ICSA programs are closely related as described in [ISASecure-119]. This document is structured in the same manner as [CSA-200]. Section 6 highlights those accreditation and operations requirements that are the same and different for CSA and ICSA.

[ICSA-100] discusses the relationship between ISASecure ICSA and the ANSI/ISA/IEC 62443 effort.

2 Normative references

2.1 General

NOTE 1 The following is the highest level document that describes the ISASecure ICSA certification program.

[ICSA-100] *ISCI IIoT Component Security Assurance – ISASecure Certification Scheme*, as specified at https://www.ISASecure.org

NOTE 2 The following is the highest level document that describes the ISASecure CSA certification program.

[CSA-100] *ISCI Component Security Assurance – ISASecure Certification Scheme*, as specified at https://www.ISASecure.org

2.2 Accreditation

2.2.1 Chartered laboratory operations and accreditation

NOTE 1 Accreditation for ISASecure CSA as described in [CSA-200] is a prerequisite to accreditation for ISASecure ICSA.

[CSA-200] *ISCI Component Security Assurance – ISASecure CSA chartered laboratory operations and accreditation*, as specified at https://www.ISASecure.org

NOTE 2 The following document can be tailored for chartered laboratories performing CSA, ICSA, SSA or SDLA certifications, or any combination of these.

[ISASecure-202] *ISCI ISASecure Certification Programs – Application and Contract for Chartered Laboratories*, internal ISCI document

2.2.2 Deleted

2.2.3 Deleted

2.3 ISASecure symbol and certificates

NOTE The following document describes the ISASecure symbol and certificates and how they are used within the ISASecure ICSA program.

[ICSA-204] *ISCI IIoT Component Security Assurance – Instructions and Policies for Use of the ISASecure Symbol and Certificates*, as specified at https://www.ISASecure.org

[ICSA-205] *ISCI IIoT Component Security Assurance – Certificate Document Format,* as specified at https://www.ISASecure.org

2.4 Technical specifications

2.4.1 General technical specifications

[ICSA-102] *ISCI IIoT Component Security Assurance – Baseline document versions and errata for ICSA 1.0.0 specifications*, as specified at https://www.ISASecure.org

NOTE The following document is the overarching technical specification for ISASecure ICSA certification.

[ICSA-300] *ISCI IIoT Component Security Assurance – ISASecure certification requirements,* as specified at https://www.ISASecure.org

[ICSA-301] *ISCI IIoT Component Security Assurance – Maintenance of ISASecure certification,* as specified at https://www.ISASecure.org

[ICSA-303] *ISASecure ICSA Sample Report*, available on request to ISCI

2.4.2 Specifications for certification elements

NOTE 1 The following document provides the technical evaluation criteria for the Vulnerability Identification Testing (VIT-IC) element of an ICSA evaluation.

[SSA-420] *ISCI System Security Assurance – Vulnerability Identification Test Specification*, as specified at https://www.ISASecure.org

NOTE 2 The following two documents provide the technical evaluation criteria for the Functional Security Assessment element (FSA-IC) of an ICSA evaluation.

[ICSA-311] *ISCI IIoT Component Security Assurance – Functional security assessment for IIoT components,* as specified at https://www.ISASecure.org

[ICSA-500] *ISCI IIoT Component Security Assurance – Selected commonly accepted security practices*, available at https://www.ISASecure.org

NOTE 3 The following two documents provide the technical evaluation criteria for the Security Development Artifacts element (SDA-IC) of an ICSA evaluation.

[ICSA-312] *ISCI IIoT Component Security Assurance – Security development artifacts for IIoT components,* as specified at https://www.ISASecure.org

NOTE 4 The [SDLA-312] and [ISDLA-312] documents contain identical information that is used for SDLA certification (SDLPA-IC). They differ in that [SDLA-312] is the reference for the SDA (Security Development Artifacts) element of CSA called SDA-C, and [ISDA-312] is the reference for the SDA element of ICSA, called SDA-IC.

[ISDLA-312] *ISCI Security Development Lifecycle Assurance – Security development lifecycle assessment for IIoT components*, as specified at https://www.ISASecure.org

[SDLA-312] *ISCI Security Development Lifecycle Assurance – Security development lifecycle assessment*, as specified at https://www.ISASecure.org

NOTE 5 The following is the highest level document that describes the related ISASecure SDLA certification program for supplier secure product development lifecycle processes.

[SDLA-100] *ISCI Security Development Lifecycle Assurance – ISASecure Certification Scheme*, as specified at https://www.ISASecure.org

[SDLA-200] *ISCI Security Development Lifecycle Assurance – ISASecure SDLA chartered laboratory operations and accreditation*

2.5 External references

External references are documents that are maintained outside of the ISASecure ICSA program and are used by the program.

2.5.1 IACS security standards

NOTE 1 [ICSA-100] describes the relationship of ISASecure ICSA to these standards.

NOTE 2 The following pairs of references that have the same document number 62443-m-n, provide the same technical standard, as published by the organizations ANSI/ISA and IEC.

[ANSI/ISA-62443-1-1] ANSI/ISA-62443-1-1 *(99.01.01)-2007 Security for industrial automation and control systems Part 1-1: Terminology, concepts and models*

[IEC 62443-1-1] IEC TS 62443-1-1:2009 *Industrial communication networks – Network and system security - Part 1-1: Terminology, concepts and models*

[ANSI/ISA-62443-4-1] ANSI/ISA-62443-4-1-2018 *Security for industrial automation and control systems Part 4-1: Secure product development lifecycle requirements*

[IEC 62443-4-1] IEC 62443-4-1:2018 *Security for industrial automation and control systems Part 4-1: Secure product development lifecycle requirements*

[ANSI/ISA-62443-4-2] ANSI/ISA-62443-4-2-2018 *Security for industrial automation and control systems Part 4-2: Technical security requirements for IACS components*

[IEC 62443-4-2] IEC 62443-4-2:2019 *Security for industrial automation and control systems Part 4-2: Technical security requirements for IACS components*

2.5.2 International standards for certification programs

NOTE The following international standards apply to the ISASecure ICSA certification and testing processes.

[ISO/IEC 17065] ISO/IEC 17065, "*Conformity assessment - Requirements for bodies certifying products, processes, and services*", September 15, 2012

[ISO/IEC 17025] ISO/IEC 17025, "*General requirements for the competence of testing and calibration laboratories*", November 2017

2.5.3 International standards for accreditation programs

[ISO/IEC 17011] ISO/IEC 17011, "*Conformity assessment – General requirements for accreditation bodies accrediting conformity assessment bodies*", November 2017

3 Definitions and abbreviations

3.1 Definitions

3.1.1
accreditation
third party attestation related to a conformity assessment body conveying formal demonstration of its competence to carry out specific conformity assessment tasks

NOTE For the ISASecure ICSA certification programs, accreditation is an assessment and recognition process via which an organization is granted chartered ICSA laboratory status.

3.1.2
accreditation body
third party that performs attestation, related to a conformity assessment body, conveying a formal demonstration of its competence to carry out specific conformity assessment

3.1.3
applicant
organization that has submitted a product or process to a chartered laboratory for evaluation for ISASecure certification

3.1.4
auditable product
hardware and/or software product such that the product or its associated development process is subject to audit, in the course of a specific chartered laboratory's planned certification activities

3.1.5
capability security level
level that indicates capability of meeting a security level natively without additional compensating countermeasures when properly configured and integrated

[SOURCE text in 62443-3-3 A.2.2]

3.1.6
component
entity belonging to an IACS that exhibits the characteristics of one or more of a host device, network device, software application, or embedded device

[SOURCE IEC 62443-4-2]

3.1.7
conformity assessment body
body that performs conformity assessment services and that can be the object of accreditation

NOTE Examples are a laboratory, inspection body, product certification body, management system certification body and personnel certification body. This is an ISO/IEC term and concept.

3.1.8
chartered laboratory
organization chartered by ASCI to evaluate products and/or processes under one or more ISASecure certification programs and to grant certifications under one or more of these programs

NOTE A chartered laboratory is the conformity assessment body for the ISASecure certification programs.

3.1.9
embedded device
special purpose device running embedded software designed to directly monitor, control or actuate an industrial process

NOTE Attributes of an embedded device are: no rotating media, limited number of exposed services, programmed through an external interface, embedded OS or firmware equivalent, real-time scheduler, may have an attached control panel, may have a communications interface. Examples are: PLC, field sensor devices, SIS controller, DCS controller.

[SOURCE IEC 62443-4-2]

3.1.10
host device
general purpose device running an operating system (for example Microsoft Windows OS or Linux) capable of hosting one or more software applications, data stores or functions from one or more suppliers

NOTE Typical attributes include filesystem(s), programmable services, no real time scheduler and full HMI (keyboard, mouse, etc.).

[SOURCE IEC 62443-4-2]

3.1.11
industrial automation and control system
collection of personnel, hardware, software and policies involved in the operation of the industrial process and that can affect or influence its safe, secure and reliable operation

[SOURCE IEC 62443-4-2]

3.1.12
IIoT (Industrial Internet of Things)
system that connects and integrates industrial control systems with enterprise systems, business processes and analytics

[SOURCE IIC The Industrial Internet of Things G8: Vocabulary V2.1]

3.1.13
IIoT device
entity that is a sensor or actuator for a physical process, or communicates with sensors or actuators for a physical process, that directly connects to an untrusted network to support and/or use data collection and analytic functions accessible via that network

NOTE 1 This definition adds detail for the purposes of the present document, to the definition from ISO/IEC FDIS 20924, 3.2.4 for IoT, which reads “entity of an IoT system that interacts and communicates with the physical world through sensing or actuating.” The 20924 definition does not specify connection to an untrusted network.

NOTE 2 Examples of IIoT devices that communicate with sensors or actuators are a PLC with an internet connection, and an IIoT integrated edge computing device (see 3.1.15).

3.1.14
IIoT gateway
entity of an IIoT system that connects one or more proximity networks and the IIoT devices on those networks to each other and directly connects to one or more untrusted access networks

NOTE 1 This definition is from ISO/IEC FDIS 20924, except that IoT is replaced by IIoT, and the qualifications “directly” and “untrusted” have been added for the purposes of this document.

NOTE 2 From [IICRA]: “The proximity network connects the sensors, actuators, devices, control systems and assets, collectively called edge nodes.”

NOTE 3 An IIoT gateway device is a type of network device (see 3.1.19).

NOTE 4 Functions hosted on an IIoT gateway device may also include data translation, processing and control.

3.1.15
IIoT integrated edge computing device
IIoT device that communicates with other IIoT devices and includes either or both of: environment for hosting application software or pre-defined application software

NOTE 1 The reader is advised that terminology usage in the IoT arena is not standardized at this time, so that other sources may use other terms for this concept.

NOTE 2 Examples of application software are analytics and data filtering. Device may include IIoT gateway functionality to transmit sensor information or derivative information to the cloud, may provide instructions to sensors, actuators, controllers, or other IIoT integrated edge computing devices, application environment may consist of virtual machines and/or a container environment, may use wired communication, or cellular or other wireless communication.

NOTE 3 An example IIoT integrated edge computing device might include sensor connections providing data for a “local” processing capability on the device, and a connection to the cloud for “remote” processing of some version of that data. In this example, the IIoT integrated edge computing device would meet 62443 definitions for network device and host (if it includes an environment for hosting application software) or software application (if it includes pre-defined applications).

3.1.16
IIoT system
system providing functionalities of Industrial Internet of Things

NOTE IIoT system is inclusive of IIoT devices, IIoT gateways, sensors, actuators, analytics and processing software together with its hardware/software environment, and related human interfaces.

[SOURCE ISO/IEC FDIS 20924, 3.2.7 (for IoT, incorporating additions to NOTE)]

3.1.17
major owner
owner of more than two percent (2%) of a business entity

NOTE This percentage is intended to exclude individuals who are owners via portfolio vehicles, and identify owners that may influence the activities of the business entity.

3.1.18
major user
organization that has or plans purchase of products whose related costs and/or usage is material to the overall operations of that organization

3.1.19
network device
device that facilitates data flow between devices, or restricts the flow of data, but may not directly interact with a control process

NOTE Typical attributes include embedded OS or firmware, no HMI, no real-time scheduler and configured through an external interface.

[SOURCE IEC 62443-4-2]

3.1.20
proximity network
network that connects the sensors, actuators, devices, control systems and assets

NOTE 1 The proximity network typically connects these nodes, as one or more clusters related to a gateway that bridges to other networks.

NOTE 2 Variant of term “proximity defined network,” in ISO/IEC TR 29181-9:2017 *Information technology — Future Network — Problem statement and requirements — Part 9: Networking of everything*, which reads “network configured among devices in close proximity, using conventional LAN or WAN technologies: which are in not only physically close proximity, but also closely related, or logically close proximity.”

[SOURCE text in [IICRA]]

3.1.21
significant financing
financing that is material to the operations of the recipient

3.1.22
significant financial interest
financial interest where the value of this interest is material to the financial position of the entity that has the interest

3.1.23
significant sales
sales that are material to the operations of the seller

3.1.24
software application
one or more software programs and their dependencies that are used to interface with the process or the control system itself (for example, configuration software and historian)

NOTE 1 Software applications typically execute on host devices or embedded devices.

NOTE 2 Dependencies are any software programs that are necessary for the software application to function such as database packages, reporting tools, or any third party or open source software.

[SOURCE IEC 62443-4-2]

3.1.25
symbol
graphic or text affixed or displayed to designate that ISASecure certification has been achieved

NOTE An earlier term for symbol is “mark.”

3.1.26
termination
withdrawal of certification, initiated by the entity that holds the certification

3.1.27
tier
designation to identify a set of certification criteria, where any two tiers are comparable under some ordering scheme

NOTE ISASecure ICSA offers certification to Core tier or Advanced tier. Advanced is the higher tier, as it encompasses more requirements than Core tier.

3.1.28
trust
confidence that an operation, data transaction source, network or software process can be relied upon to behave as expected

NOTE 1: An entity can be said to "trust" a second entity when it (the first entity) makes the assumption that the second entity will behave as the first entity expects.

NOTE 2: Trust may apply only for some specific function.

[SOURCE IEC 62443-4-2]

3.1.29
untrusted
not meeting predefined requirements to be trusted

NOTE 1 An entity may simply be declared as untrusted.

NOTE 2 A common use of this term for ICSA is in the phase “untrusted network” or “untrusted connection,” which defines the security posture assumed for networks to which a component is designed to connect, as declared by the product supplier. ([ICSA-300] requirement ICASecure_IC.R4 requires such a declaration.) Networks accessible to the public, such as the internet or cell networks to

which a component connects, are expected to be declared as untrusted. Networks to which a component connects that are identified as untrusted may also include, but are not limited to, internal enterprise networks that may not be under the full control of the asset owner responsible for the cybersecurity impact of the IIoT component. These enterprise networks may be controlled by the asset owner's overall enterprise or by another enterprise such as a partner or vendor. Some ICSA functional security requirements only apply to component interfaces declared to support direct connections to untrusted networks.

[SOURCE 62443-4-2 NOTE 2 added]

3.1.30
update
incremental hardware or software change in order to address security vulnerabilities, bugs, reliability, or operability issues

[SOURCE IEC 62443-4-2]

3.1.31
upgrade
incremental hardware or software change in order to add new features

[SOURCE IEC 62443-4-2]

3.1.32
withdrawal
cancellation of the statement of conformity

3.2 Abbreviations

The following abbreviations are used in this document.

ANSI	American National Standards Institute
ASCI	Automation Standards Compliance Institute
BS	Bachelor of Science
CACE	Certified Automation Cyber Security Expert
CACS	Certified Automation Cyber Security Specialist
CE	computer engineering
CISA	Certified Information Systems Auditor
CISSP	Certified Information Systems Security Professional
CSSLP	Certified Secure Software Lifecycle Professional
CS	computer science
CSA	component security assurance
EDSA	embedded device security assurance
FSA-IC	functional security assessment for IIoT components
GICSP	Global Industrial Cyber Security Professional
IACS	industrial automation and control system(s)
IAF	International Accreditation Forum
ICSA	IIoT Component Security Assurance
IEC	International Electrotechnical Commission
IIoT	Industrial Internet of Things
IoT	Internet of Things
ILAC	International Laboratory Accreditation Cooperation
ISA	International Society of Automation
ISCI	ISA Security Compliance Institute
ISO	International Organization for Standardization
SDA-C	security development artifacts for components
SDA-IC	security development artifacts for IIoT components
SDLA	security development lifecycle assurance
SDLPA-C	security development lifecycle process assessment for components
SDLPA-IC	security development lifecycle process assessment for IIoT components
SMA	security maintenance audit
VIT-IC	vulnerability identification testing for IIoT components

4 Background

4.1 Technical ISASecure ICSA certification elements

ISASecure ICSA is a certification program that is applicable to a subset of IACS components that meet eligibility criteria as defined in this section. An IACS component is an entity that is used to build control systems and that exhibits the characteristics of one or more of a *software application*, *embedded device*, *host device*, or *network device*. These component types are defined in the standard [IEC 62443-4-2] and in 3.1 of the present document. ICSA certification may be granted for IACS components that:

- meet the [IEC 62443-4-2] definition for at least one of embedded device, host device or network device; and
- meet the definition in Section 3.1 of this document for at least one of *IIoT device* or *IIoT gateway*.

In accordance with the definitions in 3.1, IIoT devices and IIoT gateways are intended to support direct connection to an untrusted network.

ICSA applies to physical devices only. However, if a physical device eligible for ICSA certification also includes a software application, then 62443-4-2 requirements for software applications will be part of the ICSA certification. An IIoT integrated edge computing device (3.1.15) is a type of IIoT device, hence is within the scope of ICSA certification.

ICSA certification has the following elements:

- Security Development Lifecycle Process Assessment for IIoT components (SDLPA-IC);
- Security Development Artifacts for IIoT components (SDA-IC);
- Functional Security Assessment for IIoT components (FSA-IC); and
- Vulnerability Identification Testing for IIoT components (VIT-IC).

SDLPA-IC and SDA-IC both assess development process. SDLPA-IC is an evaluation of the component supplier's secure product development lifecycle process. SDA-IC examines the artifacts that are the outputs of the supplier's secure product development lifecycle process for the component to be certified.

FSA-IC examines the security capabilities of the component. In accordance with [IEC 62443-4-2], requirements for security functionality differ based upon 62443 component type, that is, whether the component is an embedded device, host device, network device, and/or software application. The certifier determines all 62443 component types applicable to a product and whether it is an IIoT device and/or an IIoT gateway. FSA-IC then incorporates requirements for all component types applicable to the product. VIT-IC scans the component for the presence of known vulnerabilities.

The ICSA program defines two tiers of certification for an IIoT component, called Core tier and Advanced tier. Advanced tier offers an increased level of security assurance.

Both certification tiers include the certification elements listed above. SDLPA-IC does not have an associated tier. SDA-IC and VIT- IC assessments are the same for both tiers with the exception of allowable residual risk for known security issues. FSA-IC incorporates more requirements for Advanced Tier than for Core tier.

NOTE In ISDLA-312 v6.3, the treatment of residual risk related to known security issues is found in SDLA requirement SDLA-DM-4-ICSA1.

Maintenance of ICSA certification requires a periodic surveillance audit called Security Maintenance Audit (SMA), described in 6.5.3.4 below.

ISASecure ICSA certification is distinct from ISASecure CSA (Component Security Assurance) certification, which verifies conformance with 62443-4-2. [ICSA-301] describes the process for a product with CSA certification to obtain ICSA certification. At a high level, an ICSA Core tier certification requires meeting most CSA capability security level 2 certification requirements, together with some extensions to both functional and lifecycle requirements. Likewise, ICSA Advanced tier requires meeting most CSA capability security level 4 certification requirements, together with extensions to functional and lifecycle requirements. [ICSA-100] describes the relationship of ICSA with the 62443 standard; [ISASecure-119] compares ISASecure ICSA with ISASecure CSA in requirement-by-requirement detail. There is no difference between SDLPA-C for CSA and SDLPA-IC for ICSA; both require a supplier organization to hold an ISASecure SDLA process certification as a prerequisite for any product certification.

4.2 ISASecure ICSA certification program implementation

ISCI is organized as an interest area within ASCI (Automation Standards Compliance Institute), a not-for-profit 503 (c) (6) corporation owned by ISA. Descriptions of the governance and organizational structure for ASCI are found on the ISASecure website: https://www.ISASecure.org.

ASCI ICSA chartered laboratories are organizations that are accredited to evaluate components under the ISASecure ICSA program. ASCI grants accredited laboratories the right to process ISASecure ICSA certifications for components on its behalf. A chartered laboratory will issue an ISASecure ICSA certificate for a component that meets the ICSA certification requirements for its applicable component type(s), as determined by the chartered laboratory. Compliance with component certification requirements is determined based upon process audits, functional audits, and tests, which measure adherence to the ISASecure ICSA requirements for SDLPA-IC, SDA-IC, FSA-IC, and VIT-IC.

A supplier meets the SDLPA-IC criteria by holding the ISASecure SDLA process certification described in [SDLA-100]. This prerequisite for an ICSA product certification is further detailed in [ICSA-300].

All evaluations defined by the ICSA specifications are conducted directly by a chartered laboratory or its subcontractors. The list of ASCI ICSA chartered laboratories is posted on the ISCI website at https://www.ISASecure.org.

A chartered laboratory reports new certificates and updates (including suspensions, terminations, and withdrawals) to ISCI (see Requirement ICSA.R39). Certificates granted and updates are posted on the ISCI website. ISCI will post certificates and updates upon receipt from a chartered laboratory, except that for certificates granted the supplier may request that posting be delayed up to 90 days. ISCI will provide a facility via which a product user may determine if an ICSA certification has been granted, updated, suspended, terminated, or withdrawn.

NOTE A supplier might request a delay in posting a certificate granted, to achieve advantageous timing for planned announcements.

[SSA-420] requires a specific tool to be used by a chartered laboratory to perform VIT-IC.

5 Summary of operations and accreditation requirements

5.1 Overview

ISASecure ICSA will operate as an internationally recognized certification program. To meet this standard, the chartered laboratory operations and accreditation requirements are designed to comply with accepted international standards applicable to product certification and testing.

The operations of ISASecure ICSA chartered laboratories shall be in compliance with the applicable requirements in:

- [ISO/IEC 17065], the international standard that applies to bodies that certify products, processes or services, and
- [ISO/IEC 17025], the international standard that applies to test organizations.

The present document is organized using the outline of [ISO/IEC 17065]. Where required, it interprets requirements in that document for ISASecure ICSA and adds additional requirements. Of particular note are requirements for:

- Organizational and financial affiliations of chartered laboratories (6.3.3);
- Qualifications for chartered laboratory personnel (6.4.3.1);
- Content of chartered laboratory application and evaluation procedures (6.5.3.1.2 and 6.5.3.2.3)
- Directory listing of certified products (6.5.3.3);

- Appeals for client complaints (6.5.3.7); and
- Managing complaints to suppliers regarding certified products (6.6.3.6).

5.2 Accreditation process

Accreditation of a chartered laboratory for ISASecure ICSA requires as a prerequisite, accreditation for ISASecure CSA. The accreditation process for CSA is described in [CSA-200]. Further accreditation requirements consist of an assessment of the organization's implementation of the ICSA program against the general requirements in ISO/IEC 17025, 17065 and the specific requirements in Section 6 of this document, together with an assessment of technical readiness for performing ISASecure ICSA evaluations. As described in 7.3 of this document, technical readiness assessment is based upon review of laboratory processes and procedures as well as review of artifacts from SDA-IC, FSA-IC and VIT-IC evaluations carried out by the laboratory on a component. To be recognized as a chartered laboratory for the ISASecure ICSA program, a laboratory shall attain the following accreditations, performed by an IAF/ILAC accreditation body:

- Accredited to ISO/IEC 17065, with technology scope of accreditation covering ISASecure ICSA certification; and
- Accredited to ISO/IEC 17025, with technology scope of accreditation covering testing to ISASecure FSA-IC and VIT-IC specifications.

The laboratory accreditation process consists of two steps. In the first step, an IEC assessor who is qualified with respect to the above two accreditations will complete an evaluation of all accreditation requirements. Provisional chartered status is granted if ISCI's analysis of the assessor's report following this evaluation, shows that the laboratory meets the requirements for formal accreditation and technical readiness assessment defined in 7.3 of the present document. At this point the accreditation body has not yet formally granted accreditation, which requires a review and approval process internal to the accreditation body.

Once a laboratory has attained provisional chartered status, ASCI grants that laboratory the right to perform component evaluations and grant ISASecure ICSA certifications. These rights continue as long as the laboratory receives formal accreditation from an ICSA accreditation body in a timely manner (the second step) and maintains this status.

5.3 Grace period for CSA chartered laboratories to grant ICSA certifications

Organizations must hold provisional or full ICSA chartered laboratory status as described in 5.2 in order to grant ICSA certifications, with the exception of a grace period defined as follows.

- In the six months after ICSA specifications are published, any CSA accredited laboratory may grant ISCA certifications.
- Chartered laboratories that apply for ICSA accreditation in the six months after ICSA specifications are published, are permitted to grant ICSA certifications prior to obtaining ICSA provisional chartered laboratory status, until the earlier of (1) one year after the accreditation body commences ICSA accreditation assessment for the laboratory and (2) 2.5 years after the ICSA specifications are published.

As an example, if a chartered laboratory submits their application for ICSA accreditation on or before the six month mark after ICSA specifications are published, and if their accreditation body begins evaluation at the nine-month mark after ICSA publication, the laboratory may continue to grant ICSA certifications until the 21 month mark after ICSA publication, whether or not they have completed the process for provisional or full ICSA accreditation by that time. On the other hand, if for example, a chartered lab submits their application for ICSA accreditation one year after publication of the ICSA specifications, no further grace period applies after the six-month mark after ICSA publication, and the laboratory will be granted the right to grant ICSA certifications when they achieve provisional ICSA accreditation status as described in 5.2.

6 Requirements on operations of chartered laboratories

6.1 Overview

Section 6 of the present document specifies all requirements on the operation of ICSA chartered laboratories. It provides specific interpretations for ISO/IEC 17065 requirements, and defines further requirements that are specific to the ISASecure ICSA program.

Section 6 is organized as follows:

- The sub sections at numbering level 2 (6.2, 6.3, 6.4, 6.5, 6.6) each correspond to a clause in [ISO/IEC 17065], covering in turn clauses 4-8 in that document.
- Each of these sub sections in the present document has three further sub sections as follows:
    - *Overview* - provides a list of the topics covered in the corresponding clause of [ISO/IEC 17065]. This section includes an informative description of the differences between CSA and ICSA on the topics of this sub section.
    - *Scheme references for standard requirements* - A number of ISO/IEC 17065 requirements refer in turn to compliance with requirements specified by a certification scheme. This sub section in the present document provides a table that lists each such ISO/IEC 17065 requirement and provides a reference to the documentation in the ISASecure ICSA scheme where the relevant scheme requirements are found. These references may refer to ISASecure ICSA scheme documents that are listed in section 2 of the present document, or may refer to the present document itself, in particular to requirements in the sub sections in the present document described next.
    - *ISASecure ICSA specific requirements* - This sub section lists additional scheme specific requirements, beyond those derived directly from [ISO/IEC 17065] together with the other documents of the ISASecure ICSA certification scheme.

6.2 General requirements

6.2.1 Overview

Clause 4 *General requirements* in [ISO/IEC 17065] covers the following topics in associated sub clauses of that document:

- Legal and contractual matters (4.1)
- Management of impartiality (4.2)
- Liability and financing (4.3)
- Non-discriminatory conditions (4.4)
- Confidentiality (4.5)
- Publicly available information (4.6).

Informative description of delta from CSA: Among the general requirements in 6.2 of this document, the following differences are found in the ICSA program vs. the CSA program. Other requirements are the same for ICSA as for CSA, extended in scope to cover ICSA certifications.

- Certificate format
- Revisions to certificates after SMA and upon suspension/restoral

6.2.2 Scheme references for standard requirements

The following table provides scheme references, for [ISO/IEC 17065] requirements in clause 4 of that document that refer to certification scheme requirements.

Table 1 – Scheme references for ISO/IEC 17065 clause 4

ISO/IEC 17065 sub clause	ISO/IEC 17065 requirement reference	Scheme topic referenced	ISASecure ICSA reference
4.1.2 *Certification agreement*	4.1.2.2 h	Certification scheme requirements regarding client references to their certification	[ICSA-300] 5.1 requirement IC.R3, and [ICSA-204]
4.1.2 *Certification agreement*	4.1.2.2 f, g	Certification scheme requirements on actions taken by a client upon loss of certification, and on reproduction of certification documents	No unique requirements specified by scheme
4.1.2 *Certification agreement*	4.1.2.2 j	Certification scheme requirements on certification body to verify tracking of complaints received by client	[ICSA-200] 6.6.3.6
4.1.3 *Use of license, certificates and marks of conformity*	4.1.3.1	Control by the certification body, as specified by the certification scheme, of mechanisms for indicating a device is certified	Requirements on mechanisms are in [ICSA-204], which include revising ICSA certificates after supplier SMA and upon suspension/restoral (see [ICSA-200] Requirement ICSA.R39)
4.2 *Management of impartiality*	4.2.10	Period of time between performing consultancy and certification services	[ICSA-200] Requirement ICSA.R5
4.6 *Publicly available information*	4.6c)	Certification scheme requirements regarding client references to their product certification	[ICSA-300] 5.1 Requirement IC.R3, and [ICSA-204]

ISO/IEC 17065 sub clause	ISO/IEC 17065 requirement reference	Scheme topic referenced	ISASecure ICSA reference
4.6 *Publicly available information*	4.6a)	Certification scheme requirements related to granting certification	[ICSA-300]

6.2.3 ISASecure ICSA specific requirements

This sub section lists additional scheme specific requirements related to Clause 4 *General requirements* in [ISO/IEC 17065], beyond those derived from [ISO/IEC 17065] together with the other documents of the ISASecure ICSA certification scheme.

Requirement ICSA.R1 – Confidentiality for ASCI and ISCI
The general confidentiality requirement in [ISO/IEC 17065] 4.5.1 SHALL be interpreted to include the requirement that neither ASCI nor ISCI shall have access to information generated during ISASecure evaluations, except by permission of the applicant, or as required to fulfill ISCI's oversight role as scheme owner.

Requirement EDSA.R2 – Deleted

Requirement ICSA.R3 – Internal distribution for assessment reports
Procedures for report distribution internal to the chartered laboratory SHALL limit copies of test and assessment reports only to those that the chartered laboratory determines need the information to fulfill their work responsibilities.

Requirement ICSA.R4 – Public availability of ISCI complaint escalation process
The [ISO/IEC 17065] requirement 4.6d) in the sub clause 4.6 *Publicly available information* refers to procedures for handling complaints and appeals. This information SHALL include the information about complaints to ASCI/ISCI in 6.5.3.7 of this document.

Requirement ICSA.R5 – Time delay from provision of consultancy
The [ISO/IEC 17065] requirement 4.2.10 refers to the period of time between personnel having provided consultancy for a product and reviewing or making a certification decision. The minimum time period SHALL be two years.

Requirement ICSA.R6 – Notification of changes to certification requirements
The chartered laboratory SHALL have processes to keep interested parties informed of changes to certification requirements (such as changes to legal agreements associated with the certification process). Since the supplier must maintain an SDLA certification in order to maintain an existing ICSA certification over time, the certification body SHALL inform the holder of an ICSA certification regarding changes to the SDLA certification criteria, as also required by the SDLA scheme in [SDLA-200]. The certification body SHALL also inform the supplier of changes to other ICSA certification criteria, as these changes will affect certification of upgrades (as defined in 3.1.31) of a certified component in accordance with [ICSA-301], so will be required by the supplier for planning purposes.

6.3 Structural requirements

6.3.1 Overview

Clause 5 *Structural requirements* in [ISO/IEC 17065] covers the following topics in associated sub clauses of that document:

- Organizational structure and top management (5.1)
- Mechanism for safeguarding impartiality (5.2).

Informative description of delta from CSA: Among the structural requirements in 6.3 of this document, all requirements are the same for ICSA as for CSA, extended in scope to cover ICSA certifications.

6.3.2 Scheme references for standard requirements

The following table provides scheme references, for [ISO/IEC 17065] requirements in clause 5 of that document that refer to certification scheme requirements.

Table 2 – Scheme reference for ISO/IEC 17065 clause 5

ISO/IEC 17065 sub clause	ISO/IEC 17065 requirement reference	Scheme topic referenced	ISASecure ICSA reference
5.2 *Mechanism for safeguarding impartiality*	5.2.1 (Notes 2 and 3)	Certification scheme owner participation in mechanism for impartiality	No unique requirements specified by scheme
5.2 *Mechanism for safeguarding impartiality*	5.2.4 (Note 2)	Certification scheme requirements on interests represented by mechanism for safeguarding impartiality	No unique requirements specified by scheme

6.3.3 ISASecure ICSA specific requirements

This sub section lists additional scheme specific requirements related to clause 5 *Structural requirements* in [ISO/IEC 17065], beyond those derived from [ISO/IEC 17065] together with the other documents of the ISASecure ICSA certification scheme.

Additional requirements on financial and other organizational affiliations of chartered laboratories are defined as follows, to further safeguard impartiality.

Requirement ICSA.R7 – Organizational affiliations
When the separate legal entity as in [ISO/IEC 17065] 4.2.7 is a major user of certified products, the personnel of the separate legal entity shall not be involved in the management of the certification body, the review, or the certification decision.

Requirement ICSA.R8 – Financial affiliations
The following requirements apply to a chartered laboratory regarding its financial affiliations with suppliers and users of auditable products. The term "auditable product" is defined in 3.1.4. A supplier of auditable products is typically a certification client of the chartered laboratory. However, other organizations could also sell these products, and these cases are covered in this requirement as well.

- A chartered laboratory or a major owner of the chartered laboratory SHALL NOT:
    - provide significant financing to a supplier or to a major user of auditable products;
    - be a major owner of a supplier or of a major user of auditable products;

- A chartered laboratory SHALL NOT:
    - receive significant financing from a supplier or from a major user of auditable products, or their major owners;
    - have as a major owner, an organization that is a supplier or a major user of auditable products, or a major owner of such an organization;
- A person involved in the management of the certification body, the review, or the certification decision for the chartered laboratory SHALL NOT have a significant financial interest in a supplier or major user of auditable products.

Requirement ICSA.R9 – Chartered laboratory sales and purchases

The following requirements apply to a chartered laboratory regarding its sales and purchase activities:

- A chartered laboratory SHALL NOT have significant sales of any products or services to suppliers of auditable products, other than certification services;
- A chartered laboratory SHALL NOT sell auditable products;
- Prices and agreements related to any products or services that a chartered laboratory purchases from a supplier of auditable products SHALL NOT have dependencies on related certification activity.

6.4 Resource requirements

6.4.1 Overview

Clause 6 *Resource requirements* in [ISO/IEC 17065] covers the following topics in associated sub clauses of that document:

- Certification body personnel (6.1)
- Resources for evaluation (6.2)

Informative description of delta from CSA: Among the resource requirements in 6.4 of this document, the following difference is found in the ICSA program vs. the CSA program. Other requirements, including qualifications for assessors responsible for FSA, SDA, and VIT elements of those two programs, are the same for ICSA as for CSA, extended in scope to cover ICSA certifications.

- Requirement for personnel with full professional certifications (ICSA.R11)

6.4.2 Scheme references for standard requirements

The following table provides scheme references, for [ISO/IEC 17065] requirements in clause 6 of that document that refer to certification scheme requirements.

Table 3 – Scheme references for ISO/IEC 17065 clause 6

ISO/IEC 17065 sub clause	ISO/IEC 17065 requirement reference	Scheme topic referenced	ISASecure ICSA reference
6.1 *Personnel*	6.1.1.3	Certification scheme requirements to release information created during an evaluation	[ICSA-200] Requirement ICSA.R1
6.1.2 *Management of competence for personnel involved in the certification process*	6.1.2.1 a	Certification scheme requirements for competency of personnel involved in certification	[ICSA-200] 6.4.3.1
6.1.2 *Management of competence for personnel involved in the certification process*	6.1.2.1 b	Certification scheme requirements for training of personnel involved in certification	[ICSA-200] 6.4.3.1
6.2.1 *Internal resources* 6.2.2 *External resources*	6.2.1, 6.2.2.1	Applicable requirements from other standards	[ICSA-200] 6.4.3.2

6.4.3 ISASecure ICSA specific requirements

This sub section lists additional scheme specific requirements related to clause 6 *Resource requirements* in [ISO/IEC 17065], beyond those derived from [ISO/IEC 17065] together with the other documents of the ISASecure ICSA certification scheme.

6.4.3.1 Personnel qualifications

For the purposes of this section, the term “control system” refers to not only industrial discrete and process control systems, but systems in other domains of cyber-physical control such as building automation, medical devices, and automobiles, and encompasses any components (network devices, embedded devices, software applications, host devices) commonly used in a control system.

Requirement ICSA.R10 – FSA-IC, SDA-IC, and SMA auditor minimum qualifications

The [ISO/IEC 17065] requirement 6.1.2.1a) in the sub clause 6.1.1 *Management of competence for personnel involved in the certification process* refers to competencies of personnel involved in the certification process. The minimum qualifications for personnel that are responsible for evaluation to FSA-IC, SDA-IC and SMA requirements SHALL include those specified in Table 4.

The level of knowledge required for IEC 62443 as indicated in the last row of Tables 4-5, SHALL at a minimum be sufficient for the individual to prepare and present a one hour overview on the scope of application and contents of the standard, and be capable of quickly finding the answers to questions about what the standard requires on a particular topic, if given access to the text of the standard. For the other security standards and practices listed in the table, the level of knowledge required SHALL at a minimum be equivalent to 8 hours of training on the standard or practice.

Table 4 – FSA-IC, SDA-IC, and SMA auditor qualifications

Category of qualification / experience	FSA-IC auditor	SDA-IC auditor SMA auditor
Formal education	• BS Electrical Engineering **OR** • BS Computer Engineering (CE) **OR** • BS Computer Science (CS) **OR** • BS Chemical Engineering with CE or CS minor **OR** • BS Cyber Security or equivalent (such as Computing and Security Technology, Information and Network Security, Cybersecurity and Information Assurance) **OR** • Equivalent science or engineering degree **OR** • Bachelors or equivalent level degree in other subject, if individual has sufficient experience in computer technology field as specified below **OR** • Degree as described above, higher than BS **OR** • Exceed minimum criterion stated below under "Relevant development work experience." Specifically, where a minimum of 4 or 6 years experience is specified there, the individual shall have ten or more years.	• BS Electrical Engineering **OR** • BS Computer Engineering **OR** • BS Computer Science **OR** • BS Chemical Engineering with CE or CS minor **OR** • BS Cyber Security or equivalent (such as Computing and Security Technology, Information and Network Security, Cybersecurity and Information Assurance) **OR** • Equivalent science or engineering degree **OR** • Bachelors or equivalent level degree in other subject, if individual has sufficient experience in computer technology field as specified below **OR** • Degree as described above, higher than BS **OR** • Exceed minimum criterion stated below under "Relevant development work experience." Specifically, where a minimum of 4 or 6 years experience is specified there, the individual shall have ten or more years.
Professional certification	• CISA, CISSP, GICSP, CACE, CACS, or equivalent **OR** • For individuals that meet all qualifications in this column that use the term "control systems," a professional certification equivalent to one in the above list, except for any required duration of cybersecurity experience, together with a plan to achieve a full certification. See text following table for details.	• CISA, CISSP, GICSP, CSSLP, CACE, CACS, or equivalent **OR** • For individuals that meet all qualifications in this column that use the term "control systems," a professional certification equivalent to one in the above list, except for any required duration of cybersecurity experience, together with a plan to achieve a full certification. See text following table for details.

Category of qualification / experience	FSA-IC auditor	SDA-IC auditor SMA auditor
Work experience in field	• Minimum four years of work experience in computer technology field, if individual has degree in one of the specific subjects identified above, or has an equivalent science or engineering degree **OR** • Minimum eight years of work experience in computer technology field, if individual has a bachelors or equivalent level degree in other subject • Minimum three years of work experience in computer technology field if individual has Master's Degree in Cybersecurity or equivalent **OR** • Minimum two years of work experience in computer technology field if individual has PhD in Cybersecurity or equivalent	• Minimum four years of work experience in computer technology field, if individual has degree in one of the specific subjects identified above, or has an equivalent science or engineering degree **OR** • Minimum eight years of work experience in computer technology field, if individual has a bachelors or equivalent level degree in other subject **OR** • Minimum three years of work experience in computer technology field if individual has Master's Degree in Cybersecurity or equivalent **OR** • Minimum two years of work experience in computer technology field if individual has PhD in Cybersecurity or equivalent

Category of qualification / experience	FSA-IC auditor	SDA-IC auditor SMA auditor
Relevant development work experience	• Min 4 year detailed product development involvement for control systems **OR** • Min 4 years of systems integration, commissioning, or maintenance experience for control systems **OR** • Min 3 year detailed product development involvement, systems integration, commissioning or maintenance experience for control systems if individual has Master's Degree in Cybersecurity or equivalent **OR** • Min 2 year detailed product development involvement, systems integration, commissioning or maintenance experience for control systems if individual has PhD in Cybersecurity or equivalent **OR** • Min 6 years system level product test of control systems • Experience includes 2 years with security-related responsibilities **OR** • Same minimums for above activities and security responsibilities for electronic hardware/software non-control systems and pass specified ISCI-approved training **OR** • Other experience requiring interaction with any of these activities for 6 years total with 2 years security responsibilities, and pass specified ISCI-approved training, unless four years involved control systems	• Min 4 years electronic hardware or software development experience for control systems, or for non-control systems and pass specified ISCI-approved training **OR** • Other experience requiring interaction with electronic hardware or software development, integration, commissioning, maintenance for 6 years total with 2 years security responsibilities and 2 years of product development responsibilities, and pass specified ISCI-approved training, unless four years involved control systems • Demonstrates understanding and experience with defining and implementing product lifecycle process improvements • Experience includes 2 years with security-related responsibilities
Relevant auditing work experience	• Min 1 year experience performing technical product audit **OR** • 2 years in position with significant role in interaction with auditors **OR** • Min 3 years experience performing cybersecurity audit (organizational) **OR** • Min 3 years in position in organization which has been audited for cybersecurity, with significant role in interaction with auditors **OR** • Industry-recognized training in IT cybersecurity auditing **AND** • Pass specified ISCI-approved training, if qualifying based on organizational audit or IT audit training	• Min 1 year experience performing software process audit OR 2 years in position with significant role in interaction with auditors

Category of qualification / experience	FSA-IC auditor	SDA-IC auditor SMA auditor
Relevant industry specific knowledge	• General knowledge of at least two different control systems or pass specified ISCI approved training **AND** • General knowledge of application of control systems and roles and duties of employees at sites using control systems or pass specified ISCI approved training **AND** • Moderate level knowledge of networking and communication protocols **AND** • Able to independently read and interpret requirement specifications for control systems products, or for other computer technology products and pass specified ISCI approved training **AND** • Able to independently read and understand user installation and configuration documents for control systems products, or for other computer technology products and pass specified ISCI approved training **AND** • Knowledge of methods used to protect communications and detect / prevent communication attacks	• General knowledge of end-end electronic hardware or software development life cycle **AND** • General knowledge of control systems architectures or pass specified ISCI-approved training
Knowledge of security standards	• IEC 62443 Standard plus at least one of: ○ Common Criteria ○ ISO/IEC 27001 ○ IEC 61508 **AND** • If have not met a cybersecurity experience requirement under professional certification, also pass specified ISCI-approved training.	• IEC 62443 Standard plus at least one of: ○ Common Criteria ○ ISO/IEC 27001 ○ IEC 61508 **AND** • If have not met a cybersecurity experience requirement under professional certification, also pass specified ISCI-approved training.

If the individual meets all qualifications for an auditor role that use the term “control systems,” then the professional certification qualification may be initially met if the individual achieves the equivalent of a professional certification from lists shown in the above table, with the exception of any certification qualification for a minimum duration of cybersecurity experience. If the chosen certification offers formal recognition for individuals meeting all certification criteria, but without sufficient experience to achieve the full certification (for example as "Associate of ISC2" for CISSP), the individual SHALL obtain this recognition to initially satisfy this professional certification qualification.

In all cases, to remain qualified after this initial qualification is achieved, the chartered lab SHALL plan and monitor the individual’s progress toward a full professional certification equivalent to one on the specified lists. Several of these professional certification programs offer a “starter” credential that does not require experience, where the full credential may be earned later. Other programs do not have an experience requirement.

NOTE If a candidate for auditor meets all qualifications in a column of Table 4 or Table 5 that use the term “control systems,” then GICSP or a similar control-system focused professional certification is recommended.

Requirement EDSA.R11 – Deleted

Requirement ICSA.R11 – Chartered laboratory requirement for personnel with full professional certifications

Two years after a chartered laboratory receives initial CSA accreditation, all ICSA certification evaluations toward ICSA certificates issued by the chartered laboratory SHALL be performed under the technical oversight of individuals holding a relevant professional certification as specified in the second row of Table 4 or Table 5.

NOTE 1 CSA accreditation is a prerequisite for ICSA accreditation.

NOTE 2 The requirements ICSA.R10 and ICSA.R12 imply that a chartered laboratory may initiate ISCA certification operations before their auditors/evaluators have met the experience requirement for a full professional certification listed under those requirements. ICSA.R11 requires that ultimately, lead auditors/evaluators must meet these experience requirements and fully achieve one of these professional certifications.

Requirement ICSA.R12 – VIT-IC lead evaluator minimum qualifications

The [ISO/IEC 17065] requirement 6.1.2.1a) in the sub clause 6.1.1 *Management of competence for personnel involved in the certification process* refers to competencies of personnel involved in the certification process. The minimum qualifications for personnel that that are responsible for the technical aspects of VIT testing and interpretation of results shall include those specified in Table 5.

Table 5 – VIT-IC lead evaluator qualifications

Category of qualification / experience	VIT-IC lead evaluator
Formal education	• BS Electrical Engineering **OR** • BS Computer Engineering **OR** • BS Computer Science **OR** • BS Chemical Engineering with CE or CS minor **OR** • BS Cyber Security or equivalent (such as Computing and Security Technology, Information and Network Security, Cybersecurity and Information Assurance) **OR** • Equivalent science or engineering degree **OR** • 4 years work experience in testing of control systems may be substituted for degree • 4 years work experience in known vulnerability testing may be substituted for degree
Professional certification	• CISA, CISSP, GICSP, CACE, CACS, or equivalent **OR** • For individuals that meet all other qualifications for this role, a professional certification equivalent to one in the above list except for any required duration of cybersecurity experience, together with a plan to achieve a full certification. See text following Table 4 for details.
Work experience in field	• Min 4 years work experience in computer technology field
Relevant development work experience	• Min 4 year detailed product development involvement for computer technology systems **OR** • Min 4 years of systems integration, commissioning, or maintenance experience for computer technology systems **OR** • Min 3 years System Level Product Test for computer technology systems • Experience includes 1 year with software security-related responsibilities • Experience includes 2 years involvement with networking technologies
Relevant test work experience	• Min 1 year experience performing testing on computer technology systems

Category of qualification / experience	VIT-IC lead evaluator
Relevant industry specific knowledge	• Successful completion of training class or 1 year experience in job demonstrating proficiency with VIT tool to be used **AND** • Moderate level knowledge of networking and communication protocols **AND** • Able to independently read and understand user installation and configuration documents for control systems products
Knowledge of security standards	IEC 62443 Standard plus at least one of: • Common Criteria • ISO/IEC 27001 • IEC 61508

Requirement ICSA.R13 – Currency of skills and knowledge
Staff training SHALL BE kept up-to-date and staff SHALL keep up-to-date of current normative specification issues (includes participation in technical groups or committees).

6.4.3.2 Other standards

The [ISO/IEC 17065] requirements 6.2.1 *Internal resources* and 6.2.1 *External resources* in the sub clause 6.2 *Resources for evaluation* refer to compliance with applicable requirements in ISO/IEC 17025, 17020, and 17021. Accreditation to ISO/IEC 17025 is required for an ICSA chartered laboratory. Requirements from ISO/IEC 17020 which apply to inspection activities, have been adapted and incorporated in this document as follows and hence are noted but not repeated here:

Table 6 – ISO/IEC 17020 requirements specified

ISO/IEC 17020 requirement	Topic	CSA-200 requirement
6.1 6c	Continuing training	ICSA.R13
7.4.2	Test and assessment records ("Inspection records" in 17020)	ICSA.R31

6.5 Process requirements

6.5.1 Overview

Clause 7 *Process requirements* in [ISO/IEC 17065] covers the following topics in associated sub clauses of that document:

- General (7.1)
- Application (7.2)
- Application review (7.3)

- Evaluation (7.4)
- Review (7.5)
- Certification decision (7.6)
- Certification documentation (7.7)
- Directory of certified products (7.8)
- Surveillance (7.9)
- Changes affecting certification (7.10)
- Termination, reduction, suspension or withdrawal of a certification (7.11)
- Records (7.12)
- Complaints and appeals (7.13)

Informative description of delta from CSA: Among the process requirements in 6.5 of this document, the following differences are found in the ICSA program vs. the CSA program. Other requirements are the same for ICSA as for CSA, extended in scope to cover ICSA certifications.

- Document [ICSA-100] defines ICSA certification scheme, vs. [CSA-100]
- Documents [ICSA-300], [ICSA-301] define ICSA certification criteria, vs. [CSA-300], [CSA-301] for CSA
- Method for obtaining ICSA certification for component holding CSA certification
- Information required for ICSA application is desired tier, vs. desired security level for CSA
- Information required on certificate is defined in [ICSA-204], vs. [CSA-204]
- Surveillance requirement (6.5.3.4), periodic process for Security Maintenance Audit (SMA)
- Surveillance requirement impacts conditions for withdrawal of certification (6.5.3.6)
- Suspension and restoral and related actions are applicable to ICSA but not to CSA (6.5.3.6)
- Criteria for eligibility for certification (ICSA.R15)
- Document [ICSA-303] defines form of ICSA assessment report vs. [CSA-303] for CSA (ICSA.R22)

6.5.2 Scheme reference for standard requirements

The following table provides scheme references, for [ISO/IEC 17065] requirements in clause 7 of that document that refer to certification scheme requirements.

Table 7 – Scheme reference for ISO/IEC 17065 clause 7

ISO/IEC 17065 sub clause	ISO/IEC 17065 requirement reference	Scheme topic referenced	ISASecure ICSA reference
7.1 *General*	7.1.1	Certification scheme used by an ICSA chartered laboratory	Defined in [ICSA-100]
7.1 *General*	7.1.2	Refers to normative documents against which a component is evaluated	For initial certifications, documents are [ICSA-300] and its normative references; for products with a version previously certified, documents are [ICSA-301] and its normative references; [ICSA-200] ICSA.R18 specifies current versions of these documents
7.1 *General*	7.1.3	Person or committee to provide explanations per application of normative documents	ISCI Technical Steering Committee, as stated in [ICSA-200] requirement ICSA.R14
7.2 *Application*	7.2	Information that scheme requires for client application	[ICSA-300] 5.1 and 5.2 requirements IC.R1, R2 and R4 for initial certification; ICSA certification requirements for products with a version previously certified to ICSA or CSA are in [ICSA-301]
7.4 *Evaluation*	7.4.4	Evaluation of device to scope of certification and requirements specified in scheme	Certification requirements for initial certification are listed in [ICSA-300] requirement IC.R5; ICSA certification requirements for products with a version previously certified to ICSA or CSA are in [ICSA-301]

ISO/IEC 17065 sub clause	ISO/IEC 17065 requirement reference	Scheme topic referenced	ISASecure ICSA reference
7.4 *Evaluation*	7.4.9 Note 2	Whether certification scheme requires certification body to perform evaluation under its responsibility after application	Yes, per [ICSA-300] 5.2
7.7 *Certification documentation*	7.7.1 f	Information scheme requires on the document signifying certification	Certificate format and content specified in [ICSA-204] and [ICSA-205]
7.8 *Directory of certified products*	7.8 last paragraph	Information about certified products made available to a directory	[ICSA-200] 6.5.3.3, ICSA.R39
7.9 *Surveillance*		Initiate surveillance of products in accordance with the certification scheme	Security Maintenance Audit (SMA) 6.5.3.4 and [ICSA-301]
7.10 *Changes affecting certification*	7.10.1	Actions required by scheme for changes to certification criteria	[ICSA-200] Inform clients per ICSA.R6, update processes per ICSA.R18
7.11 *Termination, reduction, suspension or withdrawal of certification*	7.11.3	Actions required when a certification is terminated, suspended or withdrawn	For suspension, withdrawal and termination, see [ICSA-301] ISASecure_ICM.R2 and [ICSA-200] ICSA.R39. Reduction is not defined for ICSA certification
7.11 *Termination, reduction, suspension or withdrawal of certification*	7.11.4, 7.11.5	Scheme requirements related to suspension	Conditions to restore after suspension in [ICSA-301] Requirement ISASecure_ICM.R2. Other actions related to suspension and restoral in [ICSA-200] ICSA.R39
7.12 *Records*	7.12.3	Whether scheme requires complete re-evaluation of product on a predetermined cycle	No, as explained in [ICSA-200] 6.5.3.4

6.5.3 ISASecure ICSA specific requirements

This sub section lists additional scheme specific requirements related to clause 7 *Process requirements* in [ISO/IEC 17065], beyond those derived from [ISO/IEC 17065] together with the other documents of the ISASecure ICSA certification scheme.

6.5.3.1 Application

6.5.3.1.1 Process requirements

Requirement ICSA.R14 – Determining application of specifications
The [ISO/IEC 17065] requirement 7.1.3 in clause 7 Process *requirements* refers to persons or committees who provide the chartered laboratory with explanations as to the application of the ISASecure specifications. This role SHALL be fulfilled by the ISCI Technical Steering Committee.

Requirement ICSA.R15 – Determining applicant eligibility
The chartered laboratory SHALL be responsible for determining whether a product presented by a potential client meets the scope for an ICSA certification, and which 62443 and IIoT component type(s) apply to the product (software application, embedded device, host device, network device, IIoT device, IIoT gateway). The chartered laboratory MAY request guidance from ISCI in this matter. If the client does not concur with the decision of the chartered laboratory, they MAY use the compliant escalation process described in Requirements ICSA.R41 and ICSA.R42.

6.5.3.1.2 Content of procedures

Requirement ICSA.R16 – Application steps procedure
Procedures for processing a certification application SHALL identify the steps for the application, administrative/technical processing of the investigation in chronological order, personnel responsible for each stage of the process, and records maintained at various steps of the process.

Requirement ICSA.R17 – Maintenance of procedure for application
Procedures for developing and maintaining certification application processing procedures SHALL identify personnel responsible for developing, reviewing and maintaining the procedures, the frequency for review, and personnel responsible for verifying that the procedures are being followed.

6.5.3.2 Evaluation

6.5.3.2.1 General Process requirements

Requirement ICSA.R18 – Current ISASecure specifications
[ISO/IEC 17025] 7.2.1.3 on selection of test methods, specifies using the latest valid version of the standards upon which tests are based, where appropriate. The appropriate versions of ISASecure specifications to use for a certification SHALL be identified in accordance with transition policies and specification listings found on the ISASecure web site at https://www.ISASecure.org. The current versions of all specifications for an ISASecure program are listed in the specification numbered “102,” as in [ICSA-102] for ICSA.

Requirement EDSA.R19 – Deleted

Requirement EDSA.R20 – Deleted

Requirement ICSA.R21 – VIT-IC report
Detailed reporting on VIT-IC results for a component SHALL be carried out in accordance with the requirements on VIT-IC reporting in the technical specification for VIT-IC, which is listed in the normative references for [ICSA-300].

Requirement ICSA.R22 – Assessment report
The [ISO/IEC 17065] requirement 7.4.9 in sub clause 7.4 *Evaluation*, refers to documentation of evaluation results prior to review. This documentation SHALL at a minimum include an assessment report following the content and format of [ICSA-303], the ICSA assessment report sample. A report following this template SHALL also be provided to the client.

6.5.3.2.2 Deleted

Requirement EDSA.R23 – Deleted

Requirement EDSA.R24 – Deleted

Requirement EDSA.R25 – Deleted

Requirement EDSA.R26 – Deleted

Requirement EDSA.R27 – Deleted

6.5.3.2.3 Content of procedures

Requirement ICSA.R28 – Equipment calibration
Persons responsible for the calibration of equipment (where applicable) and authorized to perform each type of calibration SHALL be identified. Records for each calibration SHALL contain sufficient information to permit their repetition.

Requirement ICSA.R29 – Content of test or assessment methods or procedures
Each test or assessment method or procedure SHALL have sufficient detail instructions that assure reasonable repeatability of the test or assessment and include or address the: title, effective date, assessment or test data to be obtained and recorded, objective acceptance criteria for results, test or assessment techniques, where additional information to that required by the ICSA technical specifications is required to meet these goals. In addition, test procedures SHALL include or address: specific test equipment to use and instructions for handling the equipment.

Requirement EDSA.R30 – Deleted

Requirement ICSA.R31 – Content of test or assessment data sheet
Each test or assessment data sheet or similar document SHALL include the test or assessment procedure and specification used, date of the test or assessment, test or assessment report number, signature of the personnel performing the test or assessment, and test or assessment results. In addition, test data sheets shall include the product or component tested and test equipment used.

Requirement ICSA.R32 – Content of procedure maintenance procedures
Procedures for developing and maintaining test or assessment methods and procedures SHALL identify the personnel responsible for developing, reviewing and maintaining the procedures, specify frequency of review by management, ensure consistency with recognized specifications, ensure that deviations still assure the product, component or process conforms with the specification, and ensure modifications are reviewed by personnel who are familiar with the specification.

Requirement ICSA.R33 – Content of procedures for evaluating test or assessment data
Procedures for evaluating test or assessment data SHALL require the investigator to: verify and use a latest appropriate specification edition (per ICSA.R18), provide written justification of how a product, component or process complies with each section of the specification (including a reference to a test or assessment procedure), and address components not listed by the supplier.

Requirement ICSA.R34 – Content of policy for evaluation of test or assessment data
Policies on evaluation of test or assessment data SHALL identify personnel responsible for technical decisions on the specification, how to decide which section of a specification applies, how to handle newly developed technologies when the specification does not apply; require that interpretations of the specifications are documented and made readily available for the appropriate investigators; and require the resolution of product, component or process discrepancies without the laboratory engaging in the redesign, except to explain the failures in regard to the ISASecure specification.

Requirement ICSA.R35 – Content of procedures for preparing technical reports
Procedures for preparing technical reports SHALL BE written and SHALL:

- Identify personnel responsible for preparation, review of technical content, and initial or revision approval;
- Require the appropriate test and evaluation procedures; and
- Ensure that technical corrections involve qualified personnel.

6.5.3.3 Directory of certified products

The [ISO/IEC 17065] requirement 7.8 refers to certification information to be published in a directory of certifications granted by the certification body.

Requirement ICSA.R36 – Input to scheme directory
The chartered laboratory SHALL inform ISCI of each certification granted and provide a copy of the certificate, to support ISCI's central directory of ISASecure certifications.

Requirement ICSA.R37 – Accuracy of certification status
Proper controls SHALL be in place to assure accuracy of information on the certificate and in chartered laboratory records of certified entities.

6.5.3.4 Surveillance

The ISASecure ICSA certification scheme requires a periodic evaluation of the supplier's security maintenance practices as applied to products holding ICSA certification, called Security Maintenance Audit (SMA). A supplier must maintain good standing under SMA for a product in order to retain its ICSA certification. [ICSA-301] provides details of the SMA surveillance process.

Certification of updated and upgraded product versions (as defined in 3.1.30 and 3.1.31), and certification to updated ISASecure versions, are covered in [ICSA-301]. As described in [ICSA-301], maintaining ICSA certification for updates of a certified product requires maintenance by the supplier of a SDLA process certification, which in turn requires periodic recertification audits under the SDLA scheme, as described in [SDLA-300]. These audits also provide a surveillance process for ICSA.

SMA is an element of the ICSA scheme and is not part of the SDLA scheme, but SMA in many cases is performed at the same time as SDLA recertification to improve efficiency.

The ISASecure ICSA certification scheme does not require inspection of samples of actual shipped product for compliance with certification requirements. ISCI does not require a chartered laboratory to verify periodically that components shipped by the supplier that are labeled with a version number that has been certified, are in fact that version. However, ISO/IEC 17065 requires that the chartered laboratory monitor the use of the ISASecure symbol. This includes proper symbol use as it relates to product version.

6.5.3.5 Deleted

6.5.3.6 Termination, reduction, suspension or withdrawal of certification

The [ISO/IEC 17065] sub clause 7.11 refers to termination, reduction, suspension, or withdrawal of certification. Reduction is not defined for ICSA certification. The following requirements apply to termination, suspension, restoral and withdrawal.

Requirement ICSA.R38 – Suspension, restoral, withdrawal or termination of certification
An ISASecure ICSA product certification SHALL remain valid for a product and its updates, or be suspended, restored, or withdrawn in accordance with [ICSA-301] Requirement ISASecure_ICM.R2.

The certification body SHALL terminate a certification if the supplier reports to them that the product has left support status under the ISASecure SDLA-certified SDL process, or if the supplier otherwise requests termination of the certification for any reason.

If the certifier determines the supplier has not participated in good faith in the certification process, the certifier SHALL withdraw the certification.

The following requirement includes actions as referenced in [ISO/IEC 17065] sub clause 7.11.3, that are required by the scheme upon termination, suspension or withdrawal.

Requirement ICSA.R39 – Notification of certification status change and certificate updates
The chartered laboratory SHALL provide ISCI an updated certificate after each SMA (per 6.5.3.4) for a certified component, where these updates are as described in [ICSA-204]. The chartered laboratory SHALL inform ISCI of any suspension, restoral, withdrawal or termination of an ISASecure product certification at the time it occurs. In the case of suspension or restoral, the chartered laboratory SHALL at this time provide ISCI with an annotated certificate indicating suspension or restoral, where these annotations are as described in [ICSA-204]. The chartered laboratory SHALL inform the supplier that ISCI posts certificates granted and updates, upon receipt from the chartered laboratory, except that the supplier may request a delay of up to 90 days from the grant date for posting of certificates granted.

NOTE The action to terminate or withdraw a certificate that is granted, but not yet posted on the ISCI website, will not be posted by ISCI.

6.5.3.7 Complaints and appeals

The [ISO/IEC 17065] requirement 7.13.1 under 7.13 *Complaints and appeals*, refers to the certification body process related to complaints and appeals.

Requirement ICSA.R40 – Complaints regarding evaluations or certifications
A chartered laboratory SHALL be responsible for managing the resolution of complaints related to any aspect of compliance for a product it evaluated or certified.

Requirement ICSA.R41 – Escalation for complaints and appeals
The published chartered laboratory process for handling complaints SHALL include the provision that complaints may be appealed to ISCI by the party bringing the complaint, if the internal chartered laboratory resolution procedure does not offer a resolution satisfactory to them. Appealed complaints SHALL first go to the ISCI Technical Steering Committee. They MAY be further appealed to the ISCI governing board, then to the ASCI board of directors.

Requirement ICSA.R42 – Escalation for complaints and appeals related to application of specifications
An appealed complaint MAY request a ruling on whether the ISASecure specifications were correctly applied in a specific instance. Such a complaint SHALL NOT be escalated to the ASCI board of directors, but is resolved within ISCI. This ruling could impact:

- Whether the certification process is applicable to a particular product that has applied for certification;
- Whether or not a certification was granted; or

- Adequacy of the product evaluation process by the chartered laboratory.

NOTE Neither ISCI nor ASCI accept certification applications, nor process, grant, or revoke certifications. This is the role of a chartered laboratory. ISCI can assist in interpretation of the ISASecure specifications.

6.6 Management system requirements

6.6.1 Overview

Clause 8 *Management system requirements* in [ISO/IEC 17065] covers the following topics in associated sub clauses. Sub clause 8.1 describes two options open to certification bodies to meet the ISO/IEC 17065 management system requirements. Option A is the option for a certification body to comply with the management system requirements listed in sub clauses 8.2-8.8 of [ISO/IEC 17065]. Option B is the option for a certification body to comply with ISO 9001 requirements. Option B does not require that the certification body be certified to ISO 9001.

- Options (8.1)
- General management system documentation (Option A) (8.2)
- Control of documents (Option A) (8.3)
- Control of records (Option A) (8.4)
- Management review (Option A) (8.5)
- Internal audits (Option A) (8.6)
- Corrective actions (Option A) (8.7)
- Preventative actions (Option A) (8.8)

Informative description of delta from CSA: Among the management system requirements in 6.6 of this document, all requirements are the same for ICSA as for CSA, extended in scope to cover the ICSA certifications.

6.6.2 Scheme references for standard requirements

No requirements in [ISO/IEC 17065] Section 8 refer to scheme specific requirements.

6.6.3 ISASecure ICSA specific requirements

This sub section lists additional scheme specific requirements related to clause 8 *Management system requirements* in [ISO/IEC 17065], beyond those derived from [ISO/IEC 17065] together with the other documents of the ISASecure ICSA certification scheme. They apply whether the chartered laboratory elects Option A or Option B to fulfill the management system requirements.

6.6.3.1 General management system documentation

Requirement ICSA.R43 – Scope of procedures under management system
Chartered laboratory procedures SHALL cover the entire "quality loop" from application for services to final assessment or listing of certification status, including follow-up services.

Requirement ICSA.R44 – Responsibility for quality
The chartered laboratory SHALL:

- Identify the personnel responsible for quality, other general and the specific responsibilities for quality, and the authority delegated to each activity;

- Specify the coordination necessary between different activities; and
- Identify the control over activities that affect quality.

Requirement ICSA.R45 – Housekeeping
Adequate measures SHALL be taken to ensure good housekeeping at the chartered laboratory facilities where evaluation activities are performed.

Requirement ICSA.R46 – Item inventory
Laboratory procedures for handling of artifacts, or customer or laboratory equipment to be tested or used in tests, SHALL address item inventory.

Requirement ICSA.R47 – Facility security
Chartered laboratory measures and procedures related to security SHALL include provisions for: controlling access, off hours security, and fire protection for the facility; informing all personnel security policies; limiting distribution of confidential information; limiting access to and safe storage of records (including certificates and reports); back-up or off-site storage; and designate personnel responsible for monitoring security.

6.6.3.2 Control of documents

Requirement ICSA.R48 – Processing for revisions to normative specifications
Policies and procedures for distribution and control of normative specifications SHALL identify the personnel responsible for maintaining and distributing revised specifications, and a method to notify all relevant locations, including clients and agents, about modifications or amendments.

Requirement ICSA.R49 – Archival of superseded specifications
Superseded normative specifications SHALL be archived.

6.6.3.3 Control of records

Requirement ICSA.R50 – Maintenance of records
Records maintained for evaluation and certification SHALL identify the personnel responsible for maintaining records and how to correct or modify information on a record.

6.6.3.4 Management review

Requirement ICSA.R51 – Management follow-up review for deficiencies
Internal quality audit policies and procedures SHALL specify the management review of reasons for deficiencies, conclusions, recommendations on corrective actions, and the effectiveness of corrective actions.

6.6.3.5 Internal audits

Requirement ICSA.R52 – Basis for internal audits
Internal quality audit policies and procedures SHALL specify the basis for conducting audits.

Requirement ICSA.R53 – Contents included in internal audit reports
Audit reports SHALL include the name(s) of the auditor(s), the areas audited, the dates of the audit and the signature of the auditor(s), the discrepancies encountered, corrective action plan (including time for completion and evidence of implementation), and review by upper management.

Requirement ICSA.R54 – Internal audits of satellite facilities
QA oversight of company owned satellite facilities SHALL include routine and documented internal audits of satellite facility personnel, regular headquarters review and audit of the quality assurance program and audits

conducted by satellite personnel, and consistency of technical records and interpretations among all facilities.

Requirement ICSA.R55 – Implementation for permanent corrective actions
Internal quality audit policies and procedures SHALL specify how permanent changes resulting from corrective actions are recorded in standard operating procedures, instructions, manuals and specifications.

6.6.3.6 Complaints to suppliers of ICSA certified products

Requirement ICSA.R56 – Supplier process for disclosure of complaints related to noncompliance
A chartered laboratory SHALL include the following in its signed agreement with the client organization: that the client organization has a documented process for meeting the requirements regarding complaints they receive related to compliance with ISASecure product certification requirements, that are found per [ISO/IEC 17065] 4.1.2.2j. These requirements address handling and disclosure to the chartered laboratory of such complaints known to the certified organization, to the chartered laboratory.

The intent of the following broader provision is to improve the ISASecure product certification programs.

Requirement ICSA.R57 – Supplier process for disclosure of complaints related to security of ISASecure certified product
The signed agreement between the chartered laboratory and the client SHALL include the following provision. Any complaint regarding its certified product that is known to the supplier organization and that is determined to affect product security shall be brought to the attention of the chartered laboratory that granted the product certification. The laboratory shall evaluate the impact on the product conformance to the ISASecure ICSA requirements.

Requirement ICSA.R58 – Disclosure to ISCI of complaints related to ISASecure certified product
The chartered laboratory process for handling a report under Requirement ICSA.R57 SHALL include a process to advise ISCI if a modification to the ISASecure specifications should be considered based upon this event. This process SHALL be contingent upon approval from the client making the report, to disclose to ISCI any information concerning their product, whether or not it is attributed to their product.

7 Accreditation of chartered laboratories

7.1 Overview

Accreditation of a chartered laboratory for ISASecure ICSA requires as a prerequisite, accreditation for ISASecure CSA. The accreditation process for CSA is described in [CSA-200]. Accreditation of a chartered laboratory further involves an assessment of the organization against the requirements in the following documents:

- ISO/IEC 17065 [ISO/IEC 17065]
- ISO/IEC 17025 [ISO/IEC 17025]
- Section 6 this document, all ISASecure specific requirements subsections
- Section 7 of this document, which describes technical readiness assessment.

Technical readiness assessment is based upon review of documented laboratory processes and procedures as well as review of artifacts from sample audits carried out by the laboratory on a component, as described in Section 7.3. To be recognized as a chartered laboratory for the ISASecure ICSA program (beyond the initial grace period defined in 5.3), a laboratory shall attain the following accreditations, performed by an IAF/ILAC recognized accreditation body:

- Accredited to IAF ISO/IEC 17065, with technology scope of accreditation covering ISASecure ICSA certification; and

- Accredited to ISO/IEC 17025, with technology scope of accreditation covering ISASecure ICSA FSA-IC and VIT-IC specifications.

This internationally recognized accreditation shall be obtained by a laboratory within 18 months of obtaining provisional ICSA chartered laboratory status, as described in Section 5.2. The following section discusses requirements for attaining provisional chartered laboratory status.

7.2 Provisional chartered laboratory status

Provisional chartered laboratory status allows an organization to begin certification activities before accreditation has been formally granted by an ICSA accreditation body. Formal granting of the accreditation can occur several months after the evaluation of the laboratory has taken place and results submitted by the evaluators to the board within the ICSA accreditation body that makes the final accreditation decision.

ASCI will grant a laboratory provisional chartered status based on the results of an evaluation of the laboratory by qualified assessors for ISO/IEC 17065 and ISO/IEC 17025. Provisional chartered status is granted if the evaluation shows that the organization complies with:

- All ISO/IEC 17065 and ISO/IEC 17025 requirements;
- All numbered ISASecure specific requirements in the present document; and
- Those technical readiness criteria in Table 8 that may be verified based upon process and procedure documentation evidence. These criteria are in rows 1-3 Table 8.

The accreditation body will assess the remaining technical readiness criteria once the chartered laboratory is operating and has examples of product evaluation results available.

The evaluation for a candidate chartered laboratory is performed by an assessor that has been qualified by an IAF/ILAC recognized accreditation body. A candidate organization shall apply for accreditation as required by the accreditation body. A candidate chartered laboratory also applies to ASCI using the form [ISASecure-202]. “Provisional” chartered laboratory status is a term applied by ASCI/ISCI within the ISASecure program and is not recognized or managed by the accreditation body.

During the period when a chartered laboratory is operating in provisional status, ASCI shall be made aware of the laboratory’s expectations for receipt of formal internationally recognized accreditation by an IAF/ILAC organization. ASCI shall have the option to perform an interim review and update its evaluation for provisional status of the chartered laboratory 6 months after it is received. Once a chartered laboratory has achieved accreditation by an IEC 17011 accreditation body, that accreditation body determines the requirements and frequency for maintenance audits to maintain accredited status.

7.3 Technical readiness assessment

For technical readiness for ICSA, the accreditor verifies that the organization is accredited for ISASecure CSA or has provisional chartered laboratory status from ICSI for ISASecure CSA, and has processes and procedures in place for surveillance, termed Security Maintenance Audit (SMA) under the ICSA program. It then focuses on detail differences between ICSA and CSA for security development artifacts (SDA), functional security requirements (FSA), and pass/fail criteria for vulnerability identification testing (VIT). The evaluation consists of assessment of evidence supplied by the candidate laboratory per the evaluation criteria in Table 8.

Table 8 – Evidence for technical readiness

ID	Evidence supplied by candidate laboratory	Evaluation criteria
1	Certificate of CSA accreditation posted on public website by ISCI, OR approval of provisional CSA chartered laboratory status from ISCI director	• Accredited as CSA chartered laboratory, OR have provisional CSA chartered laboratory status
2	VIT-IC processes/procedures	• Comply with [ICSA-300] ISASecure_IC.R5 on criteria for VIT-IC pass
3	Surveillance process/procedures related to Security Maintenance Audit	• Comply with ICSA requirements in [ICSA-301] Section 5 and ISASecure_ICM.R2
4	Intermediate artifacts, paperwork and final evaluation report for a sample component covering SDA-IC, FSA-IC, and VIT-IC.	• SDA-IC artifacts unique to ICSA (meaning, different from those for CSA) were obtained as required by specifications • Results of FSA-IC indicate compliance with FSA procedures and specifications unique to ICSA • Report from VIT-IC evaluation indicates compliance with pass/fail criteria in [ICSA-300] ISASecure _IC.R5 • Evaluation report meets requirement ICSA.R22 in this document

Bibliography

[IICRA] Industrial Internet Consortium Reference Architecture, available at https://www.iiconsortium.org/pdf/IIRA-v1.9.pdf

[ISASecure-119*] ISA Security Compliance Institute - Comparison of IIoT Component Security Assurance and Component Security Assurance Certifications*, available at https://www.ISASecure.org